Gemeinsam
SICHER
DIGITAL

www.happyworx.de

Checkliste zu den Vorgaben der DSGVO

Diese Checkliste gibt Ihnen einen kurzen Überblick über die **Vorgaben der DSGVO** und zeigt Ihnen auf, in welchen Bereiche die DSGVO Einfluss hat. Weiterhin werden die notwendigen Maßnahmen aufgezeigt, damit Ihr **Unternehmen in Zukunft datenschutzkonform** agieren kann.

Wenn Sie **alle Vorgaben** eindeutig mit **JA** (Ankreuzen) beantworten können, haben Sie alles richtig gemacht. Ihre Kunden und deren Daten sind in **sicheren Händen bei Ihnen**!

Andernfalls besteht nun **Handlungsbedarf**. Gerne unterstützen wir Sie hierbei. Rufen Sie einfach bei uns durch und wir besprechen kostenfrei alle weiteren Schritte.

happyXworx

E-Mail Adresse
info@happyworx.de
Website URL

☐ Es wurden alle aktuellen Prozesse identifiziert, bei denen personenbezogene Daten verarbeitet werden.

Der Grundsatz der DSGVO lautet „Jede Datenverarbeitung muss rechtmäßig erfolgen, anhand festgelegter Zwecke, transparent, in möglichst geringem Umfang […]".

Dokumentieren Sie daher, welche personenbezogenen Daten in Ihrem Unternehmen anfallen. Darunter muss auch notiert werden, wo diese anfallen (z. B. CRM-System), in welchem Umfang (Name, Adresse, …), zu welchem Zweck (z. B. Kundenkontakt) und wie lange diese gespeichert werden (Zeitraum).

Aufgrund der Übersichtlichkeit und Ordnung, bietet sich hierbei die Nutzung eines sortierten Verzeichnis an, welche alle Datenverarbeitungsprozesse beinhaltet.

☐ Es wurden alle notwendigen Verträge zur Auftragsdatenverarbeitung (AVV) mit externen Partnern (Dienstleistern) aktualisiert oder neu abgeschlossen.

Mit allen Dienstleistern, bei denen personenbezogene Daten ausgetauscht werden, muss ein Vertrag zur Auftragsdatenverarbeitung geschlossen werden. Ist nicht ersichtlich, welche Daten wozu ausgetauscht werden, drohen hohe Geldstrafen.

Setzen Sie sich mit allen kooperierenden Dienstleistern zusammen und überarbeiten Sie die bestehenden AVV oder schließen Sie gemeinsam einen neuen AV-Vertrag.

DSGVO-Checkliste

☐ Geklärt, ob eine Datenschutzfolgeabschätzung benötigt wird und diese gegebenenfalls erstellt?

Immer dann, wenn eine Datenverarbeitung für die Rechte und Freiheiten einer Person ein hohes Risiko zur Folge hat, muss vor deren Einführung eine sogenannte DFSA erstellt und ermittelt werden, welche Folgen eine geplante Verarbeitung für den Schutz der Daten Betroffener hätte.

Vor der Ausführung der kritischen Tätigkeiten müssen Sie prüfen, ob eine DFSA notwendig ist und diese eventuell erstellen bzw. erweitern.

☐ Alle Formulare und Einwilligungserklärungen wurden überprüft?

Bevor personenbezogene Daten verarbeitet werden, muss zwangsläufig die Einwilligung der entsprechenden Person eingeholt werden?

Überprüfen Sie daher, ob die Person vor dem Absenden persönlicher Daten auf Ihre Rechte aufgeklärt wurde. (alle Kontaktformulare und sonstige Erklärungen)

Ein Beispiel kann die Erweiterung eines Kontaktformulars um eine Einwilligungs-Checkbox sein.

☐ Anpassen der Datenschutzerklärung

Die Datenschutzerklärung ist der erste Anlaufpunkt für Webseitenbesucher:In. Diese Erklärung legt übersichtlich dar, welche Daten zu welchem Zweck, wie lange und wo aufgehoben werden.

Prüfen Sie daher, ob die Datenschutzerklärung Ihrer Website den aktuellen Vorgaben der DSGVO und TT-DSG einhält.

☐ Es wurden alle Technisch organisatorischen Maßnahmen (TOM) kontrolliert oder erstellt.

TOM sind unterschiedliche Vorkehrungen, die im Unternehmen getroffen werden müssen, um die Sicherheit der erhobenen und verarbeiteten personenbezogenen Daten zu gewährleisten. Ein Beispiel kann der automatische Log-Out aus Systemen nach einer definierten Zeit sein.

Aktualisieren Sie das Verarbeitungsverzeichnis zu allen bestehenden TOM und führen Sie eventuell neue TOM ein, die eine sichere Verarbeitung der personenbezogenen Daten sicherstellen.

☐ Es ist definiert, wie mit Anfragen Betroffener umgegangen wird, die Ihre Rechte bezüglich Ihrer personenbezogenen Daten nutzen.

Jeder Besucher:In oder Person, die mit Ihrem Unternehmen in Kontakt steht, besitzt Betroffenenrechte, die er wahrnehmen kann. Bei einer Anfrage sollte klar definiert werden, wie diese Rechte vom Unternehmen ausgeführt werden.

Erstellen Sie ein klar definiertes Vorgehen, wie mit Anfragen Betroffener umgegangen wird. Stellen Sie sicher, dass die Person kurzfristig alle seine gespeicherten Daten erhalten kann, eine Lösung oder Korrektur seiner Daten möglich ist und wie mit Widersprüchen umgegangen wird.

☐ Auf Cookies und extern eingebundene Ressourcen wurde auf der Website hingewiesen und um Einwilligung erfragt.

Bisher musste nur auf die Nutzung von Cookies hingewiesen werden. Seit der Überarbeitung der DSGVO im Dezember 2021, ist diese Verordnung jedoch expliziter geworden. Jeder Besucher muss nun seine Einwilligung explizit erteilen.

Prüfen Sie daher, welche Cookies gespeichert werden und welche externen Ressourcen der Besucher laden muss, um Ihre Webseite zu nutzen. Fragen Sie ihn vor der Nutzung um explizite Einwilligung oder verzichten auf Cookies und externe Inhalte, wie Google Fonts.

☐ Es wurde geprüft, ob ein Datenschutzbeauftragter (DSB) benötigt wird und ist gegebenenfalls bestellt.

Der DSB ist der erste Ansprechpartner zu Fragen zum Thema Datenschutz. Sowohl intern als auch extern. Er ist zwar nicht verantwortlich für die Durchführung der Vorgänge, ist aber für Schulungen und Kontrolle zuständig.

Prüfen Sie, ob ein DSB bei Ihnen im Unternehmen benötigt wird und bestellen Sie einen internen oder externen DSB.

☐ Ein Reaktionsplan für Datenpannen wurde eingeführt und ist aktuell.

Auf bei bester Sensibilisierung und Prophylaxe kann es jedoch zu Fehlern oder Datenpannen kommen. In solchen Fällen, muss schnell gehandelt werden, damit der Schaden auf ein Minimum begrenzt wird.

Erstellen Sie daher einen Reaktionsplan, mit dem Sie alle notwendigen Schritt anhand einer Checkliste abarbeiten können, um alle Schäden so gering, wie möglich zu halten. Nur so ist es möglich, dass Pannen und Fehler innerhalb von 72 Stunden, den Behörden gemeldet werden können.

☐ Die Mitarbeiter:Innen werden regelmäßig im Umgang mit Daten geschult.

Social Engineering ist einer der häufigsten Gründe, dass persönliche Daten über unternehmensgrenzen Hinweg fließen. Hierbei geben Mitarbeiter:Innen direkt oder auch indirekt sensible Daten „freiwillig“ an den Täter. Mitarbeiter:Innen müssen daher auf die Gefahren, Pflichten und Rechte zum Thema Datenschutz und Datensicherheit geschult werden.

Stellen Sie sicher, dass alle Mitarbeiter:Innen immer wieder geschult werden und das Thema Datenschutz nicht stiefmütterlich im Unternehmen gehandhabt wird. Lassen Sie passende Schulungen durch einen Datenschutzbeauftragten durchführen.

PROBLEME BEIM ANKREUZEN?

Wir helfen Ihnen bei der Umsetzung aller Punkte und begleiten Sie gerne als externer Datenschutzbeauftragter.

DAMIT SIE ZEIT FÜR IHRE KUNDEN HABEN

(+49) 5121 9347 173

info@happyworx.de